PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-004037
(43)Date of publication of application : 09.01.1990

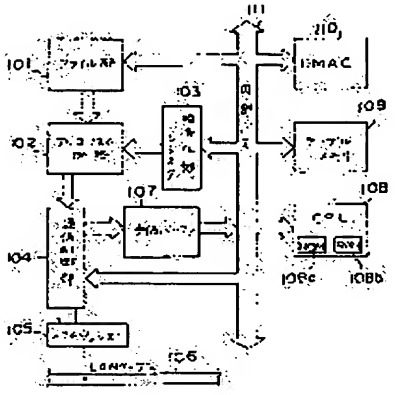
(51)Int.Cl. H04L 9/06
H04L 9/14

(21)Application number : 63-152270
(22)Date of filing : 22.06.1988

(71)Applicant : CANON INC
(72)Inventor : ARAKAWA TADASHI

(54) LAN ENCIPHERMENT SYSTEM

(57)Abstract:
PURPOSE: To increase the security effect of information by enciphering a file from a file server and outputting it onto a LAN by means of an encipherment corresponding to a user to give a file access request.
CONSTITUTION: When a file access packet from an arbitrary terminal on the LAN is inputted through a driver/receiver 105 and a communication control 104 to a receiving buffer 107, a CPU 108 confirms a file name. Next, a user identifier is known, and an access right to the file name is checked. When the check is passed, an enciphering key to be uniquely decided by the user ID is set to an enciphering key register 103. There, the CPU 108 starts a file transfer. The file is enciphered through an algorithm circuit 102, made into a packet by the communication control 104 and made to flow onto a LAN cable 106 by adding the address of the opposite party to it.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Japanese Publication for Unexamined Patent Application No. 4037/1990 (*Tokukaihei* 2-4037)

A. Relevance of the Above-identified Document

This document has relevance to claims 1, 17, and 18 of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−4037

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開
H 04 L 9/06 9/14		7240−5K　H 04 L 9/02　Z	平成2年(1990)1月9日

審査請求　未請求　請求項の数 1　(全5頁)

⑭発明の名称　LAN暗号化方式

⑳特　願　昭63−152270
㉒出　願　昭63(1988)6月22日

㉒発明者　荒川　忠　東京都大田区下丸子3丁目30番2号　キヤノン株式会社内
㉑出願人　キヤノン株式会社　東京都大田区下丸子3丁目30番2号
㉔代理人　弁理士　大塚　康徳　外1名

(57)【要約】
〔目的〕フアイルアクセス要求を出したユーザに対応する暗号化によつて，フアイルサーバからフアイルを暗号化してＬＡＮ上へ出力することにより，情報のセキユリテイ効果を高める。
〔構成〕ＬＡＮ上の任意端末からのフアイルアクセスパケツトがドライバ／レシーバ１０５，通信制御１０４を通り，受信バツフア１０７に入ると，ＣＰＵ１０８はフアイル名を確認する。次に，ユーザ識別子を知り，フアイル名へのアクセス権をチエツクする。チエツクがパスすると，ユーザＩＤにて一意的に決まる暗号化鍵を暗号化鍵レジスタ１０３へセツトする。そこで，ＣＰＵ１０８はフアイル転送を開始する。フアイルはアルゴリズム回路１０２を通つて暗号化され，通信制御１０４でパケツト化され，相手アドレスを付加してＬＡＮケーブル１０６上へ流される。

【LAN 暗号化 方式 フアイル アクセス 要求 出し 利用者 対応 暗号化 フアイル サーバー フアイル 出力 情報 安全 効果 高める 任意 端末 パケツト ドライバ レシーバ 通信 制御 通り 受信 バツフア 入り CPU フアイル名 確認 利用者 識別 子 知り アクセス権 チエツク パス 利用者 ID 一意的 暗号化鍵 レジスタ セツト フアイル 転送 開始 アルゴリズム 回路 相手 アドレス 付加 LAN ケーブル】

(2)

1

【特許請求の範囲】

ファイルサーバにおいて暗号化を行うＬＡＮ暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別する識別手段と、

該ユーザ識別子に対応して所定の暗号化鍵を記憶する暗号化鍵記憶手段と、

該暗号化鍵記憶手段から読み出された暗号化鍵に対応して暗号化を行う暗号化手段とを備え、ＬＡＮからのファイルアクセス要求に対して、前記ファイルサーバは、該ファイルアクセス要求を出したユーザに対応する暗号化により、ファイルをＬＡＮ上へ出力することを特徴とするＬＡＮ暗号化方式。

2

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-4037

⑤Int. Cl.[5]	識別記号	庁内整理番号	㊸公開 平成2年(1990)1月9日
H 04 L 9/06 9/14			
		7240-5K H 04 L 9/02	Z

審査請求 未請求 請求項の数 1 (全5頁)

㊹発明の名称　LAN暗号化方式

㉑特　願　昭63-152270
㉒出　願　昭63(1988)6月22日

㉒発明者　荒川　忠　東京都大田区下丸子3丁目30番2号　キヤノン株式会社内
㉑出願人　キヤノン株式会社　東京都大田区下丸子3丁目30番2号
㉔代理人　弁理士　大塚　康徳　外1名

明　細　書　暗号化方式。

1．発明の名称

LAN暗号化方式

2．特許請求の範囲

ファイルサーバにおいて暗号化を行うLAN暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別する識別手段と、

該ユーザ識別子に対応して所定の暗号化鍵を記憶する暗号化鍵記憶手段と、

該暗号化鍵記憶手段から読み出された暗号化鍵に対応して暗号化を行う暗号化手段とを備え、

LANからのファイルアクセス要求に対して、前記ファイルサーバは、該ファイルアクセス要求を出したユーザに対応する暗号化により、ファイルをLAN上へ出力することを特徴とするLAN

3．発明の詳細な説明

［産業上の利用分野］

本発明はＬＡＮ（ローカルエリアネットワーク）の暗号化方式に関するものである。

［従来の技術］

ＬＡＮにおいては、高速の共通通信路上に位置する各装置に媒体アクセス制御機能が分散され、各装置は対等の関係にあつて、同報機能．任意の装置間通信．通信路上の各種資源の共有等が実現されている。更に、データファイルも基本的には共有であるが、そのデータファイルが、例えば学生の成績．病院のカルテ．企業の経理情報・人事情報・マル秘文書等のいわゆる機密情報・個人情報に対しては、セキュリティの確保がなされている。

これが、ユーザ識別子（ＩＤ：認識ラベル）の導入及びデータファイル等のアクセスレベルの設定とグループ化とによるアクセス権の制限である。この方式により不正アクセスの未然防止がなされ、現在のＬＡＮシステムでは一般的に採用されている。

［発明が解決しようとする課題］

しかしながら、共通通信路を流れる信号を直に盗聴することはどこでも可能なため、データ盗用の完全なる防止をアクセス権の制限だけで行うには無理がある。従つて、共通通信路上の信号が暗号化されることが、セキュリティ対策上最良といえる。しかし、暗号化アルゴリズムと暗号化鍵／復号化鍵をＬＡＮユーザに随便に提供できるＬＡＮ暗号化方式は存在しなかつた。

又、機密情報．マル秘情報等セキュリティの強化を要する情報の更新の多くはＬＡＮ以外の場所で行われ、その後データベースの形でＬＡＮ上に位置するファイルサーバに供給され、端末ユーザに開放される。

本発明は、前記従来の欠点及び上記の点に鑑み、ファイルサーバからの出力時にデータが暗号化されるＬＡＮ暗号化方式を提供する。

又、本発明は、ファイルアクセスユーザは各ユーザ毎の専用復号化鍵を所有することを可能としたものである。

［問題点を解決するための手段］

この課題を解決するために、本発明のＬＡＮ暗号化方式は、ファイルサーバにおいて暗号化を行うＬＡＮ暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別する識別手段と、該ユーザ識別子に対応して所定の暗号化鍵を記憶する暗号化鍵記憶手段と、該暗号化鍵記憶手段から読み出された暗号化鍵に対応して暗号化を行う暗号化手段とを備える。

［作用］

かかる構成において、ＬＡＮからのファイルアクセス要求に対して、前記ファイルサーバは、該ファイルアクセス要求を出したユーザに対応する暗号化により、ファイルをＬＡＮ上へ出力する。

［実施例］

第４図は本実施例のシステム構成図であり、本実施例におけるファイルサーバの位置付けを表している。同図において、４０１-1～４０１-Nは端末を表わし、４０２はファイルサーバ（ＦＳ）、４０３はファイルサーバ更新用端末、４０４はゲートウエイ（ＧＷ）である。端末４０１-1～４０１-N、ファイルサーバ４０２、

ゲートウエイ４０４はＬＡＮ４０７で結ばれている。４０５は公衆網、４０６はＬＡＮ４０７外の端末である。ファイルサーバ４０２はＬＡＮ４０７内の端末４０１-$_1$～４０１-$_n$からアクセスされるとともに、ゲートウエイ４０４を介して公衆網に接続された端末４０６からもアクセスされることを示している。

第１図はファイルサーバ４０２内のハードウエアブロック図の１例を示したものである。図中、１０１はデータベースとしてのファイル部であり、１０２は暗号化を行うアルゴリズム回路、１０３は暗号化鍵を格納する暗号化鍵レジスタ、１０４はパケットの生成・分解等を行う通信制御部、１０５はドライバ／レシーバであり、ＬＡＮケーブル１０６につながる。１０７は受信バッファ、１０８は全体を制御するＣＰＵで処理手順を格納するＲＯＭ１０８ａと補助記憶用のＲＡＭ１０８ｂとを有する。１０９はテーブル情報が格納されるテーブルメモリ、１１０はＤＭＡコントローラ（ＤＭＡＣ）、１１１は内部バスである。

この構成における本実施例の動作を、第２図に示すフローチャートに従つて説明する。

ＬＡＮ上の任意の端末からのファイルアクセスパケットがドライバ／レシーバ１０５，通信制御部１０４を通り、受信バッファ１０７に入ると、ＣＰＵ１０８はパケットを解析し、ステップＳ１でファイルアクセスパケットであることを確認するとともにアクセス対象となるファイル名を確認する。次にステップＳ２でパケットのユーザ識別子フィールドからユーザ識別子を知り、ステップＳ３でそのファイル名へのアクセス権を、ファイルのディレクトリ情報に含まれる属性とユーザ識別子との比較によりチエックする。

チエックがパスしたら、ステップＳ４でユーザＩＤにて一意的に決まる暗号化鍵をテーブルメモリ１０９から入手し、暗号化鍵レジスタ１０３へセットする。テーブルメモリ１０９内のユーザ識別子と暗号化鍵の一例を第３図に示す。暗号化鍵レジスタ１０３の出力はアルゴリズム回路１０２に入力されており、従つてステップＳ４にてアルゴリズム回路１０２はステップＳ２で確認されたユーザＩＤ専用の暗号回路として動作する。

次にＣＰＵ１０８は、ステップＳ５でＤＭＡＣ１１０にそのファイル名のアドレスとバイト長とをセットし、ファイル転送を開始する。ファイル部１０１のファイル群から出力されたファイルは、アルゴリズム回路１０２を通り暗号化され通信制御部１０４でパケット化され、相手アドレスを付加されてドライバレシーバ１０５を通つてＬＡＮケーブル１０６上へ流れていく。ファイル転送が終了すると、ステップＳ６からステップＳ７に進んで、暗号化鍵レジスタ１０３をリセツトしてファイルサーバ４０２の動作は終了する。このリセット値は暗号化鍵のデフォルト値となり、第３図で示したテーブルに暗号化鍵が記載されていない場合に、用いられる暗号化鍵となる。

ＬＡＮ上を流れる暗号化された信号は、要求元の端末にて受信される。その端末を操作しているユーザは、ユーザ識別子で決まる自分専用の復号化鍵を用いることにより復号化が可能となる。以上で各ユーザ毎に割付けられた暗号化鍵で暗号化された信号にてファイルサーバからアクセス

ユーザに要求ファイルが届けられたここになる。

以上説明したように、暗号化鍵とユーザ識別子の対応テーブルをファイルサーバ内に保持することにより、鍵の情報交換のわずらわしさを不用とした簡易な暗号化処理が可能となり、セキュリテイの高いＬＡＮシステムが構築できるという効果がある。

［発明の効果］

本発明により、ファイルサーバからの出力時にデータが暗号化されるＬＡＮ暗号化方式を提供できる。

又、ファイルアクセスユーザが各ユーザ毎の専用復号化鍵を所有することが可能となつた。

4．図面の簡単な説明

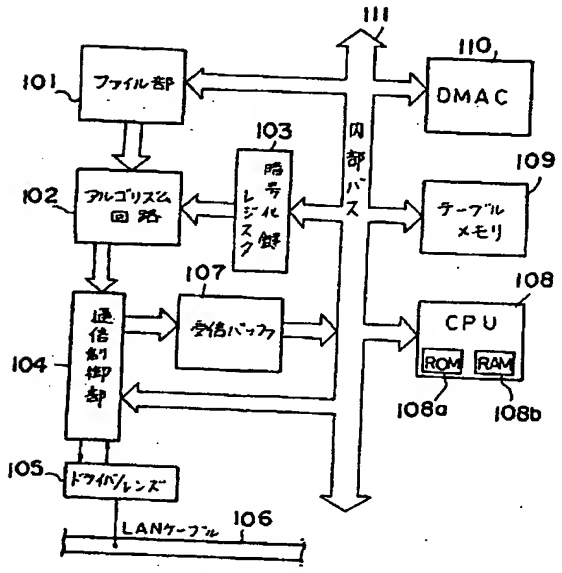
第１図は本実施例の主要部をなすファイナルサーバのハードウエアブロック図、

第２図は本実施例のファイルサーバの動作フローチヤート、

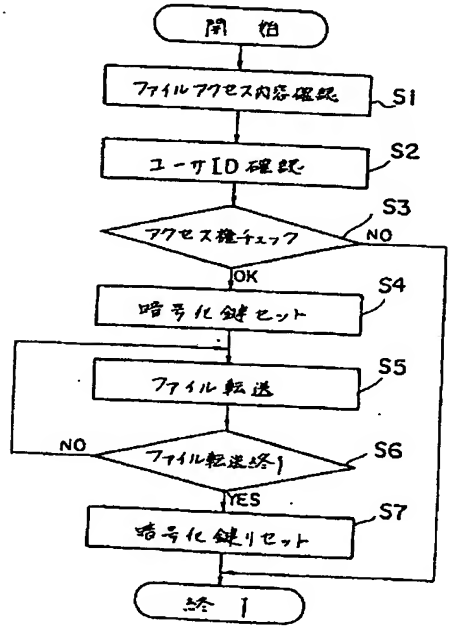
第３図はファイナルサーバ内テーブルメモリのデータ配置を表わす図、

第４図は本実施例のＬＡＮシステムの構成図である。

図中、４０１-1～４０１-n，４０３，４０６…端末、４０４…ゲートウエイ、４０２…ファイルサーバ、４０５…広域網、４０７…ＬＡＮ、１０１…ファイル部、１０２…アルゴリズム回路、１０３…暗号化鍵レジスタ、１０４…通信制御部、１０５…レシーバ／ドライバ、１０６…ＬＡＮケーブル、１０７…受信バッファ、１０８…ＣＰＵ、１０８ａ…ＲＯＭ、１０８ｂ…ＲＡＭ、１０９…テーブルメモリ、１１０…ＤＭＡＣ、１１１…内部バスである。



第１図



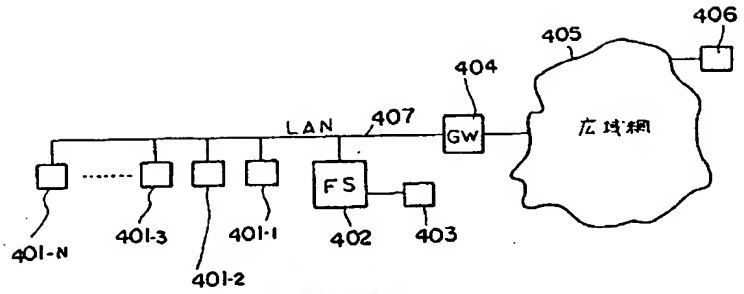
第２図

(7)

109

ユーザID	暗号化鍵
AAA	o b c
BBB	b c d
CCC	c d e
⋮	⋮

第 3 図



第 4 図